Set Up

Setting Up Single-Node Intersight Connected Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Connected Virtual Appliance setup:

Step 1 On the **Intersight Appliance Installer** screen, select **Intersight Connected Virtual Appliance** and click **Start**.

Step 2 Log in to the Intersight Virtual Appliance Connect page using your Cisco ID. If you do not have a Cisco ID, you can create one here.

a. **(Optional)** Click **Settings** to enable HTTPS Proxy Settings.

If an HTTP/S proxy is required to connect your Cisco Intersight Virtual Appliance to the internet, you must configure proxy settings before you can complete the connection step.

- Click **Settings** and enable the **HTTPS Proxy** option.
- Add the **Proxy Hostname** or **IP Address**, and the **Proxy Port**.

  The proxy port must be in the range between 1 and 65535. You can edit the Proxy settings from the appliance UI, **System** > **Settings** > **NETWORKING** > **Cloud Connection**.

b. Use the **Device ID** and **Claim Code** that is displayed on the Connect page to complete connecting to Intersight.

c. Ensure that the **Connection** status displays **Claimed**.

Note A new browser tab appears to display the status of the target claim in Intersight. If you do not have an Intersight account, you can create one in the **Account Creation** window and claim a target. If the target connection is successful, a success message is displayed. Click **Close** to exit the tab and return to the **Intersight Appliance Installer** setup wizard. If the target claim is unsuccessful, you will be taken to the Intersight login screen to restart target claim workflow.

Step 3 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Connect**—Click **Continue** to proceed to the **Check Network Requirements** step.

b) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if any of the DNS test fails, you cannot proceed with the configuration.

c) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Select Software Version** step.

d) **Select Software Version**—You have the option to download the latest version of the appliance software, or you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

a) To download the latest version of the appliance software, select the **Download Latest Version** button and click **Finish** to proceed to the **Installation Result** screen.

b) To upload a version of the appliance software, select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to manually update, install, or restore Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 15 and Downloading Software Packages for Intersight Virtual Appliance, on page 15.

- For Local Machine, browse to where you saved the software image, and then click **Finish** to proceed to the **Installation Result** screen.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish** to proceed to the **Installation Result** screen.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied

- **Port**—TCP port to use
- **Location**—Directory where the file to be copied is stored
- **Filename**—Name of the file to be copied from the network share
- **Username**—Username for authenticating with the network share
- **Password**—Password for authenticating with the network share

c) **Installation Results**—You can view the progress of the installation on this screen.

Step 4 Specify **Data Collection**.

Specify your preference to allow Intersight to send additional system information to Cisco. This option is enabled by default. For more information about what data is collected by Intersight, see Data Collected from Intersight Connected Virtual Appliance.

Step 5 Click **Register License**.

Obtain a license registration token from Cisco Smart License Manager, and apply add the token to activate your license. The license registration process could take a few minutes to complete. For more information about registering your Intersight license, watch Cisco Intersight Licensing Tiers and Registration.

After you click **Finish**, the Intersight Connected Virtual Appliance dashboard displays.

What to do next

Once you have successfully completed the initial set up of the single-node Intersight Virtual Appliance, you can add additional nodes to create a multi-node cluster. For more information, see Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 6.

Setting Up Single-Node Intersight Private Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Private Virtual Appliance setup:

Step 1 On the **Intersight Appliance Installer** screen, select **Intersight Private Virtual Appliance** and click **Start** to proceed with setting up a single-node Private Virtual Appliance.

The **Upload Software** page displays. You can upload any supported version of the software that is the same as the installer version or greater than the installer version.

Step 2 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if any of the DNS test fails, you cannot proceed with the configuration.

b) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Upload Software** step.

c) **Upload Software**—You can upload any supported version of the software that is the same as the installer version or greater than the installer version.

Select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to complete an Intersight Private Virtual Appliance deployment, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 15 and Downloading Software Packages for Intersight Virtual Appliance, on page 15.

- For Local Machine, browse to where you saved the software image, and then click **Finish** to proceed to the **Installation Result** screen.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish** to proceed to the **Installation Result** screen.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored
  - **Filename**—Name of the file to be copied from the network share
  - **Username**—Username for authenticating with the network share
  - **Password**—Password for authenticating with the network share

d) **Installation Results**—You can view the progress of the installation on this screen.

Step 3 Log in to the Intersight Virtual Appliance Connect page. Use **admin** as the username, and enter the password that you set during the installation process.

Step 4 Complete the **Register License** process.

a. Use the Reservation Request Code that you obtain on this page to generate Reservation Authorization Code in Cisco Smart Software Manager.

b. Copy the Reservation Authorization Code that you generated in **Cisco Smart Software Manager** and paste it in the Reserve License page.

c. Click **Install**.

The license reservation process can take a few minutes to complete. For information about Intersight licensing tiers and registration, watch Cisco Intersight Licensing Tiers and Registration.

After you click **Close**, the Cisco Intersight Private Virtual Appliance dashboard displays.

What to do next

Once you have successfully completed the initial set up of the single-node Intersight Virtual Appliance, you can add additional nodes to create a multi-node cluster. For more information, see Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 6.

Setting Up Intersight Assist

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Assist setup:

Step 1 1. On the **Intersight Appliance Installer** screen, select **Intersight Assist** and click **Start**.

Step 2 Log in to the Intersight Virtual Appliance Connect page using your Cisco ID. If you do not have a Cisco ID, you can create one here.

a. (Optional) Click **Settings** to enable HTTPS Proxy Settings.

If an HTTP/S proxy is required to connect your Cisco Intersight Virtual Appliance to the internet, you must configure proxy settings before you can complete the connection step.

- Click **Settings** and enable the **HTTPS Proxy** option.
- Add the **Proxy Hostname** or **IP Address**, and the **Proxy Port**.

  The proxy port must be in the range between 1 and 65535. You can edit the Proxy settings from the appliance UI, **System** > **Settings** > **NETWORKING** > **Cloud Connection**.

b. Use the **Device ID** and **Claim Code** that is displayed on the Connect page to complete connecting to Intersight.

c. Ensure that the **Connection** status displays **Claimed**.

Note A new browser tab appears to display the status of the target claim in Intersight. If you do not have an Intersight account, you can create one in the **Account Creation** window and claim a target. If the target connection is successful, a success message is displayed. Click **Close** to exit the tab and return to the Intersight Virtual Appliance setup wizard. If the target claim is unsuccessful, you will be taken to the Intersight login screen to restart target claim workflow.

Step 3 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Connect**—Click **Continue** to proceed to the **Check Network Requirements** step.

b) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if the DNS test fails, you cannot proceed with the configuration.

c) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Installations Results** screen.

d) **Installation Results**—You can view the progress of the installation on this screen.

Configuring a Multi-Node Cluster for Intersight Virtual Appliance

A multi-node cluster for Intersight Virtual Appliance allows for high availability, increased stability, and better resilience. Once you have completed the initial set up of the single-node appliance on VMware vSphere, you can add additional nodes. After you successfully add two additional nodes, you can create a multi-node cluster for Intersight Virtual Appliance.

Note Note that multi-node cluster configuration is supported only on VMware vSphere installations.

Important Once you have set up a multi-node cluster for Intersight Virtual Appliance, you cannot revert back to the single-node instance.

Requirements:

- You can set up a multi-node cluster for the appliance **only** after you have completed the initial set up of the single-node appliance. Ensure that you have set up single-node Intersight Virtual Appliance software as per the instructions in the following tasks:
  - Setting Up Single-Node Intersight Connected Virtual Appliance
  - Setting Up Single-Node Intersight Private Virtual Appliance
- You can set up a multi-node cluster at any time after you have completed the initial set up of your appliance.
- The first node must be in an **Operational** status to be able to add additional nodes for creating a multi-node cluster in Intersight Virtual Appliance.

To set up a multi-node cluster for Connected Virtual Appliance and Private Virtual Appliance, do the following:

Step 1 Access your VM using the <<https://myhost2.mydomain.com/ URL.

Step 2 On the **Intersight Appliance Installer** screen, click the **Add Node to Appliance** tab.

Step 3 On the **Add Node to Appliance** page, enter the details for the following fields, and click **Finish**.

- **Appliance Hostname/IP Address**—The hostname or the IP address of the existing stand-alone appliance to which the node will be added.
- **Appliance Username**—The admin username of the existing stand-alone appliance.
- **Admin User Password**—The admin password for the existing stand-alone appliance.

After the second node (node2) is successfully added, it is ready to join the cluster.

At this point, you can add a third node (node3) so that you can create a cluster.

Step 4 Repeat the instructions in Steps 1, 2, and 3 to add node3.

Step 5 Once the node3 has been successfully added, click **Go to Appliance Portal** to proceed to the appliance.

Step 6 Log into <<https:// myhost1.mydomain.com>>.

Step 7 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Appliance**.

Ensure that node2 and node3 are in the **Ready to Join** state.

Step 8 Click **Create Cluster**.

Important The action of creating a cluster is irreversible.

Note that the Appliance will switch to a maintenance mode while the cluster creation workflow is being executed. Allow 5-10 minutes for the progress page to load, after which you can view the progress of cluster creation on the **Multi-Node Cluster Creation Results** page. You can also view the progress of cluster creation on node2 and node3 which is available right away.

When the set up completes, the login screen appears.

Step 9 Log into the **Intersight Virtual Appliance Connect** page.

Use **admin** as the username and enter the password that you set during the initial single-node appliance setup. At this point, you can log into node2 and node3 as well.

Multi-node cluster will be fully operational when one node goes down. The appliance automatically stabilizes when one node is down. During the transition stage, your appliance might not be accessible.

When two nodes go down, the multi-node cluster will move to maintenance mode. During this state, the system will not be operational.

When the nodes come up, the multi-node cluster becomes **Operational** automatically.

Migration Path for Existing Single-Node Deployment to Multi-Node Cluster Configuration

To expand an existing single-node Intersight Virtual Appliance deployment to a multi-node cluster configuration, do the following:

1. Create a backup of your appliance.

   For more information, see Creating a Backup.

2. Restore Intersight Virtual Appliance.

For more information, see Recovering Intersight Connected Virtual Appliance and Recovering Intersight Private Virtual Appliance .

After you have successfully completed configuring the multi-node cluster for your existing single-node deployment, use the information in the following links to perform additional configuration for the multi-node cluster.

- Single Sign-on
- SSL Certificates

Recovering Intersight Connected Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

To restore a Connected Virtual Appliance configuration, you can recover the data from a backup file during the initial setup.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Installer Options** screen appears and allows you to complete the setup for either a new install or to recover the appliance software from backup.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the recovery.

Use these instructions to recover the configuration from a backup file:

Step 1 On the **Installer Options** screen, select the **Recover from Backup** tab and click **Start**.

Step 2 On the **Select Backup** page, select the protocol and enter details of the remote server from where you want to recover the backed up data.

- **Protocol**—Communication protocol option used in the backup process. Intersight Virtual Appliance currently supports SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) for backup.
- **Server IP/Hostname**—The host from which backed up data is recovered
- **Port**—TCP port on the backup server
- **Location**—Directory where the backup files are saved
- **Filename**—Name of the backup file to restore
- **Username**—Username for authenticating the backup client to the backup server
- **Password**—Password for authenticating the backup client to the backup server

Step 3 Click **Next**.

Important **The restore process cannot be modified once it has started.**

Step 4 Click **Continue** on the warning pop-up.

Step 5 On the **Select Software Version** page, you have the option to download the latest version of the appliance software, or you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

a) To download the latest version of the appliance software, select the **Download Latest Version** button and click **Finish**.

b) To upload a version of the appliance software, select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to manually restore Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 15 and Downloading Software Packages for Intersight Virtual Appliance, on page 15.

- For Local Machine, browse to where you saved the software image, and then click **Finish**.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish**.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored
  - **Filename**—Name of the file to be copied from the network share
  - **Username**—Username for authenticating with the network share
  - **Password**—Password for authenticating with the network share

You can view the progress of the recovery on the **Recovery Results** page. After the recovery process is complete, the Cisco Intersight Connected Virtual Appliance dashboard is displayed.

What to do next

For Recovering Multi-Node Cluster Deployments: If you are recovering from a back-up for a multi-node cluster deployment, first recover node1 and then add two additional nodes to create a multi-node cluster by following the steps in Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 6.

Recovering Intersight Private Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

To restore a Private Virtual Appliance configuration, you can recover the data from a backup file during the initial setup.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Installer Options** screen appears and allows you to complete the setup for either a new install or to recover the appliance software from backup.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the recovery.

Use these instructions to recover the configuration from a backup file:

Step 1 On the **Installer Options** screen, select the **Recover from Backup** tab and click **Start**.

Step 2 On the **Select Backup** page, select the protocol and enter details of the remote server from where you want to recover the backed up data.

- **Protocol**—Communication protocol option used in the backup process. Intersight Virtual Appliance currently supports SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) for backup.
- **Server IP/Hostname**—The host from which backed up data is recovered
- **Port**—TCP port on the backup server
- **Location**—Directory where the backup files are saved
- **Filename**—Name of the backup file to restore
- **Username**—Username for authenticating the backup client to the backup server
- **Password**—Password for authenticating the backup client to the backup server

Step 3 Click **Next**.

Important **The restore process cannot be modified once it has started.**

Step 4 Click **Continue** on the warning pop-up.

Step 5 On the **Select Software Version** page, you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

Note In order to manually restore Intersight Private Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 15 and Downloading Software Packages for Intersight Virtual Appliance, on page 15.

- For Local Machine, browse to where you saved the software image, and then click **Finish**.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish**.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored

- **Filename**—Name of the file to be copied from the network share
- **Username**—Username for authenticating with the network share
- **Password**—Password for authenticating with the network share

You can view the progress of the recovery on the **Recovery Results** page. After the recovery process is complete, the Cisco Intersight Private Virtual Appliance dashboard is displayed.

What to do next

For Recovering Multi-Node Cluster Deployments: If you are recovering from a back-up for a multi-node cluster deployment, first recover node1 and then add two additional nodes to create a multi-node cluster by following the steps in Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 6.

Replacing a Node in the Multi-Node Cluster for Intersight Virtual Appliance

When a node in a multi-node cluster becomes **Impaired** or the status is **Unknown**, you can replace the defective node by adding another node to the existing cluster.

To replace a defective node in an existing cluster, do the following:

Step 1 Log into a node in your multi-node cluster that is operational.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Appliance**.

Step 3 In the table under **Node**, do the following:

a. In the row of the node that either displays the **Impaired** or **Unknown** status, click on the **ellipses**.

b. Click **Replace Node**.

The status for this node now displays as **Out of Service**.

Step 4 Power-off and delete the defective node from the VMware vSphere, Microsoft Hyper-V server, or KVM hypervisor installation.

Step 5 Deploy a fresh OVA using the same DNS Domain value as the defective node.

For more information about installing and deploying the appliance, see the installation chapter.

Step 6 Access your VM using the <https://*fqdn-of-your-appliance*.com> URL.

Step 7 On the **Installer Options** screen, click the **Add Node to Appliance** tab.

Step 8 On the **Add Node to Appliance** page, enter the details for the following fields, and click **Finish**.

- **Appliance Hostname/IP Address**—The hostname or the IP address of the existing appliance VM to which the node will be added.
- **Appliance Username**—The admin username of the existing appliance VM.
- **Admin User Password**—The admin password for the existing appliance VM.

After the node is successfully added, it is ready to join the cluster.

Step 9 Log into one of the operational nodes.

Step 10 Click **Go to Appliance Portal** of the operational node and proceed to the appliance.

Step 11 Navigate to **Settings** icon > **Settings** > **General** > **Appliance**.

Step 12 In the row of the node that is ready to join the cluster, do the following:

a. Click on the ellipses.

b. Click **Join Cluster**.

c. On the pop-up screen, click **Join**.

You can monitor the progress of the workflow. Once the workflow runs successfully, the replaced node becomes completely operational.

High Availability and Disaster Recovery for Cisco Intersight Virtual Appliance

Cisco Intersight Virtual Appliance supports migration architectures for High Availability (HA) and Disaster Recovery (DR).

The following requirements must be met to successfully migrate Intersight Virtual Appliance.

- Intersight Virtual Appliance has a Fully Qualified Domain Name (FQDN). To migrate Intersight Virtual Appliance, the FQDN (hostname) of the appliance must remain the same. However, the IP address and DNS/NTP of the appliance can be changed during the recovery process.
- You can migrate the appliance from one site to another as long as the FQDN is reachable from the claimed end-point. This allows the back-up taken from one site to be restored on another site.
- Network connectivity between Intersight Virtual Appliance and its managed endpoints must be maintained.

High Availability for Intersight Virtual Appliance

You can leverage any vendor-provided solution to provide High Availability (HA) capabilities in Intersight Virtual Appliance.

Intersight Virtual Appliance deployed on VMware vSphere — Intersight Virtual Appliance supports VMware High Availability to ensure non-disruptive operation of the appliance. For more information about VMware HA, refer to the relevant documentation on VMware's website.

Intersight Virtual Appliance deployed on Microsoft Hyper-V Server — Intersight Virtual Appliance supports Microsoft Hyper-V High Availability to ensure non-disruptive operation of the appliance. Microsoft Hyper-V offers the Failed-Over Clustering High Availability solution to protect the workloads running on the host servers, thereby protecting the appliance. Failover Clustering feature allows users to experience minimum disruptions in service. For more information about Microsoft Hyper-V HA, refer to the relevant documentation on Microsoft's website.

Intersight Virtual Appliance deployed on KVM Hypervisor — KVM is supported by multiple Operating Systems (OS) vendors. The most common OS vendors are Red-Hat Virtualization and Ubuntu. For specific solutions for High Availability, refer to the documentation provided by the OS vendor.

Disaster Recovery for Intersight Virtual Appliance

For disaster recovery, you can use the existing Backup and Restore functionality in Intersight Virtual Appliance or other third-party solutions.

Backup and Restore in Intersight Virtual Appliance

Cisco strongly recommends taking periodic backup of Intersight Virtual Appliance.

For information on backing up Intersight Virtual Appliance, see Backing Up Data.

For information on restoring Intersight Connected Virtual Appliance, see Recovering Intersight Connected Virtual Appliance.

For information on restoring Intersight Private Virtual Appliance, see Recovering Intersight Private Virtual Appliance.

Third-Party Disaster Recovery Solutions

For disaster recovery configuration of the virtual machine, you can use any vendor-provided solutions to augment the DR capabilities. Refer to the vendor-specific documentation for configuration details.

VMware DR Solutions

- **VMware Snapshots** — In addition to the Intersight Virtual Appliance Backup and Restore functionality, VMware also provides VM snapshot for preserving the state and data of the virtual machine. Preserving the state includes the VM's power state, and preserving data includes all the files including the disk, memory, and other devices' virtual network interface cards. It is highly recommended that you power-off the appliance (VM) before you take the VM snapshot. For more information about VM snapshot, refer to the relevant documentation on the VMware website.
- **Intersight Virtual Appliance deployed on VMware vSphere** — VMware provides multiple solutions for DR:
  - VMware-SRM (VMware Site Recovery Manager)
  - VMware-VRS (VMware vSphere Replication)

Microsoft Hyper-V DR Solutions

Microsoft Hyper-V includes a set of built-in features that provides an efficient VM disaster recovery. Hyper-V virtual machine DR can be performed either by backing up or replicating VMs. Both options have certain aspects that should be considered when creating a DR plan. For more information, refer to the relevant documentation on the Microsoft website.

KVM Hypervisor DR Solutions

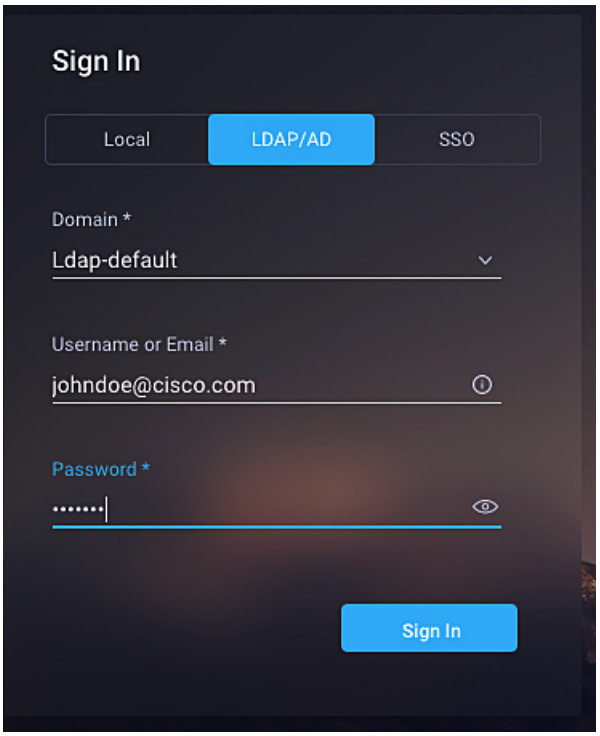
KVM is supported by multiple Operating Systems (OS) vendors. The most common OS vendors are Red Hat Virtualization and Ubuntu. For DR-specific solutions for Intersight Virtual Appliance deployed on KVM, refer to the documentation provided by the OS vendor.

For other approved Third-Party DR solutions, refer to the installation document of the Third-Party.

Logging In to Intersight Virtual Appliance

Logging In to Intersight Virtual Appliance

After installing Intersight Virtual Appliance, you can log in to the appliance as a user in one of the methods detailed below. The LDAP/AD and SSO tabs appear after you configure LDAP settings or SSO for the account.



- **Local User**—Use **admin** as the username, and use the same password that you set at the time of registering the appliance. If the password you set at the time of registering is weak, Intersight prompts you to change your password to a stronger one. After a successful reset to a strong password, you are directly logged into the appliance. Intersight supports only one local user (admin).
- **LDAP/AD**—Select the LDAP domain that you have configured, enter a **Username** or **Email** and the password that you have set up on the LDAP server. The username you use to log in must be the same as the **sAMAccountName** that you configure for the user in the LDAP server. For more information see LDAP Configuration, Add Users, and Add Groups.
- **SSO**—Enter the email ID that you have used to set up SSO in the Identity Provider. Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. For more information about SSO, see Setting up SSO.

For Local User Only —If the local user login fails as a result of an incorrect username or password, details of the failed login information will be logged in Audit Logs. You will be able to view the details of the failed login, in Audit Logs, after you successfully log in to the appliance.

Creating an Appliance Account for Downloading Software Packages

In order to complete an Intersight Private Virtual Appliance deployment, or manually update Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the Intersight Virtual Appliance, Hyperflex, or Cisco UCS Director software packages.

Note It is highly recommended that you check the Appliance Account regularly for updates and remain on the latest version of the Intersight Virtual Appliance software as it is continuously improved to include new features and enhancements. It is also important to note that only "N-3" software versions of the product are supported, with "N" being the latest version of appliance software.

Ensure that the version of the software that you are manually uploading for installation is always higher than the running version.

Use the steps in this task to create an Appliance Account:

Step 1 Log in to https://www.intersight.com/pvapp using your Cisco ID. If you do not have a Cisco ID, you can create one here.

Note: You will need to log in to https://www.intersight.com/pvapp only for creating an Appliance Account. After you have created the Appliance Account, you can access it by logging into Intersight.

Step 2 Accept the offer description and click **Next**.

Step 3 Enter a name for the Appliance Account in the **Appliance Account Creation** screen.

Step 4 Click **Create**.

After the Appliance Account is successfully created, you can log into Intersight to access the account and download the required Intersight Private Virtual Appliance, HyperFlex, or Cisco UCS Director software packages.

To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.

Note Account Administrators can enable users and groups to be able to access any of the Appliance Accounts that have been created. For more information on how to add users and groups, see Adding a User and Adding a Group.

Downloading Software Packages for Intersight Virtual Appliance

Use the steps in this task to download Intersight Virtual Appliance, Cisco Hyperflex, and Cisco UCS Director software packages.

Note To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.

Before you begin

Ensure that you have created an Appliance Account. If you have not created an Appliance Account, see Creating an Appliance Account for Downloading Software Packages, on page 15.

Step 1 Log into Intersight using your Cisco ID. If you do not have a Cisco ID, you can create one here.

Step 2 Select the account that you created for accessing the Appliance Account.

The Software Download page is displayed. You can download the required software packages from the list displayed on this page.

You can proceed to upload the software on to the appliance. For more information, see Uploading Software Packages for Intersight Private Virtual Appliance, on page 16.

After uploading the software packages, you can install them on the claimed targets. To upgrade connector packs on Cisco UCS Director targets, see Upgrading Connector Packs on UCS Director Instances.

Note The ESXi software package is also downloaded as part of the Hyperflex software package. Hence, you do not have to download a separate ESXi software package.

Uploading Software Packages for Intersight Private Virtual Appliance

Intersight Private Virtual Appliance is intended for environments where you operate data centers in a disconnected (air gap) mode. Hence, you must download software packages from either the Cisco Software Central site or by accessing the Appliance Account on Intersight, and then uploading them on to the appliance.

Use this procedure to upload software packages for your Private Virtual Appliance.

Before you begin

Ensure that you have downloaded the required software packages as follows:

- To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.
- To download Cisco HyperFlex, Cisco UCS Director or Intersight Private Virtual Appliance software packages, you will need to access your Appliance Account. For more information, see Creating an Appliance Account for Downloading Software Packages, on page 15 and Downloading Software Packages for Intersight Virtual Appliance, on page 15.

Step 1 From the left navigation panel, click **Software Repository** > **Software**.

Step 2 Click **Upload Software**.

The Upload Software page is displayed.

a) Select either **Local Machine** or **Network Share**, depending on where you saved the software packages, and then click **Next**.

b) For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file.

- **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
- **Server IP/Hostname**—The network share server from where the file is copied
- **Port**—TCP port to use
- **Location**—Directory where the file to be copied is stored
- **Filename**—Name of the file to be copied from the network share
- **Username**—User name for authenticating with the network share
- **Password**—Password for authenticating with the network share

You can track the upload progress by clicking on the **Requests** icon. When the upload process completes successfully, the software that you uploaded will appear on the Software Repository page.